University of Toronto – MAT246H1-S – LEC0201/9201

Concepts in Abstract Mathematics

Problem Set n°3

Jean-Baptiste Campesato

Due on March 12th, 2021

You can only use the material covered in class up to lecture 12 (i.e. Chapters 1, 2, 3 and 4 up to section 5 included).
Write your solutions concisely but without skipping important steps.
Make sure that your submission is readable on Crowdmark.

Exercise 1.
Let p be a prime number. Prove that

$$\forall s \in \mathbb{N} \setminus \{0\},\ \forall n \in \mathbb{N} \setminus \{0\},\ \forall x_1, \dots, x_n \in \mathbb{Z},\ \left(\sum_{k=1}^{n} x_k\right)^{p^s} \equiv \sum_{k=1}^{n} x_k^{p^s} \pmod{p}$$

Exercise 2.
The following questions are independent.

1. For which $n \in \mathbb{N}$, is $5^n - 3^n$ a prime number?
2. For which $n \in \mathbb{N}$, is $2^{2^n} + 5$ a prime number?

Exercise 3.

Solve for $x, y \in \mathbb{N} \setminus \{0\}$, $\sum_{k=1}^{x}(k!) = y^2$.

Exercise 4.
Let p be a prime number and $n \in \mathbb{N}$ satisfying $1 \leq n \leq p-1$.
Prove that $(p-n)!(n-1)! \equiv (-1)^n \pmod{p}$.

Sample solution to Exercise 1.
Method 1:
Let's prove the statement by induction on $s \geq 1$.

- *Base case at $s = 1$:*
  Let $n \in \mathbb{N} \setminus \{0\}$ and $x_1, \ldots, x_n \in \mathbb{Z}$.
  By Fermat's theorem we have:
  - $\left(\sum_{k=1}^{n} x_k\right)^p \equiv \sum_{k=1}^{n} x_k \pmod{p}$, and,
  - For $k = 1, \ldots, n$, $x_k^p \equiv x_k \pmod{p}$.

  Thus $\left(\sum_{k=1}^{n} x_k\right)^p \equiv \sum_{k=1}^{n} x_k \pmod{p} \equiv \sum_{k=1}^{n} x_k^p \pmod{p}$
- *Induction step:* assume that the statement of the question holds for some $s \geq 1$.
  Let $n \in \mathbb{N} \setminus \{0\}$ and $x_1, \ldots, x_n \in \mathbb{Z}$.
  Then

$$\begin{aligned}
\left(\sum_{k=1}^{n} x_k\right)^{p^{s+1}} &= \left(\left(\sum_{k=1}^{n} x_k\right)^{p^s}\right)^p \\
&\equiv \left(\sum_{k=1}^{n} x_k^{p^s}\right)^p \pmod{p} \quad \text{by induction hypothesis} \\
&\equiv \sum_{k=1}^{n} \left(x_k^{p^s}\right)^p \pmod{p} \quad \text{by the case } s = 1 \\
&\equiv \sum_{k=1}^{n} x_k^{p^{s+1}} \pmod{p}
\end{aligned}$$

Method 2:
Lemma. Let's first prove by induction on s that $\forall s \in \mathbb{N} \setminus \{0\}$, $\forall x \in \mathbb{Z}$, $x^{p^s} \equiv x \pmod{p}$.

- *Base case at $s = 1$:* Let $x \in \mathbb{Z}$ then $x^p \equiv x \pmod{p}$ by Fermat's theorem.
- *Induction step:* assume that the statement of the question holds for some $s \geq 1$.
  Let $x \in \mathbb{Z}$ then

$$\begin{aligned}
x^{p^{s+1}} &= \left(x^{p^s}\right)^p \\
&\equiv x^p \pmod{p} \text{ by the inductive hypothesis} \\
&\equiv x \pmod{p} \text{ by Fermat's theorem}
\end{aligned}$$

Which proves the lemma.

Let's prove the statement of the question:
Let $s \in \mathbb{N} \setminus \{0\}$, $x_1, \ldots, x_n \in \mathbb{Z}$ then

$$\begin{aligned}
\left(\sum_{k=1}^{n} x_k\right)^{p^s} &= \sum_{k=1}^{n} x_k \quad \text{by the lemma} \\
&= \sum_{k=1}^{n} x_k^{p^s} \quad \text{by the lemma}
\end{aligned}$$

Sample solution to Exercise 2.

1. If $n = 0$ then $5^0 - 3^0 = 0$ is not prime.
   If $n = 1$ then $5^1 - 3^1 = 2$ is prime.
   If $n > 1$ then $5^n - 3^n \equiv 1^n - 1^n \pmod 2 \equiv 0 \pmod 2$. Thus $5^n - 3^n$ is even but $5^n - 3^n > 2$, therefore it is not prime.
   Conclusion: $5^n - 3^n$ is prime for $n = 1$ only.

2. If $n = 0$ then $2^{2^0} + 5 = 2^1 + 5 = 7$ is prime.
   If $n \geq 1$ then $2^{2^n} + 5 \equiv (-1)^{2^n} + 2 \pmod 3 \equiv 1 + 2 \pmod 3 \equiv 0 \pmod 3$ (*since* 2^n *is even as* $n \geq 1$).
   Therefore $3|2^{2^n} + 5$ but $2^{2^n} + 5 > 3$. Thus $2^{2^n} + 5$ is not prime.
   Conclusion: $2^{2^n} + 5$ is prime for $n = 0$ only.

Sample solution to Exercise 3.
We first compute $y^2 \pmod 5$ in terms of $y \pmod 5$:

$y \pmod 5$	0	1	2	3	4
$y^2 \pmod 5$	0	1	4	4	1

We treat several cases.

1. Let $x = 1$ then $\displaystyle\sum_{k=1}^{x}(k!) = 1$.
   The unique $y \in \mathbb{N} \setminus \{0\}$ such that $y^2 = 1$ is $y = 1$.

2. Let $x = 2$ then $\displaystyle\sum_{k=1}^{x}(k!) = 1! + 2! \equiv 3 \pmod 5$.
   So there exists no $y \in \mathbb{Z}$ such that $\displaystyle\sum_{k=1}^{2}(k!) = y^2$ by the above table.

3. Let $x = 3$ then $\displaystyle\sum_{k=1}^{x}(k!) = 1! + 2! + 3! = 9$.
   The unique $y \in \mathbb{N} \setminus \{0\}$ such that $y^2 = 9$ is $y = 3$.

4. Let $x \geq 4$.
   Note that for $k \geq 5$, we have $5|k!$.
   Thus $\displaystyle\sum_{k=1}^{x}(k!) \equiv 1! + 2! + 3! + 4! \pmod 5 \equiv 33 \pmod 5 \equiv 3 \pmod 5$.
   So there exists no $y \in \mathbb{Z}$ such that $\displaystyle\sum_{k=1}^{x}(k!) = y^2$ when $x \geq 4$, by the above table.

So the solutions are $(x, y) = (1, 1)$ and $(x, y) = (3, 3)$.

Sample solution to Exercise 4.
Let p be a prime number and $n \in \mathbb{N}$ satisfying $1 \leq n \leq p - 1$.
Note that

$$\begin{aligned}(p-1)! &= (p-n)!(p-(n-1))(p-(n-2))\cdots(p-1)\\ &\equiv (p-n)!(-(n-1))(-(n-2))\cdots(-1) \pmod p\\ &\equiv (p-n)!(-1)^{n-1}(n-1)(n-2)\cdots 1 \pmod p\\ &\equiv (p-n)!(-1)^{n-1}(n-1)! \pmod p\end{aligned}$$

Since, by Wilson's theorem, $(p-1)! \equiv -1 \pmod p$, we get that $(p-n)!(-1)^{n-1}(n-1)! \equiv -1 \pmod p$ and thus, multiplying both side by $(-1)^{n-1}$, that $(p-n)!(n-1)! \equiv (-1)^n \pmod p$.